
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE
trustedci.org

# Cybersecurity to Enable Science: Hindsight and Vision from the NSF Cybersecurity Center of Excellence

**Von Welch**
Director, Trusted CI
PI, ResearchSOC
Director, IU CACR

NCSA - May 30th, 2019

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Trusted CI:
# The NSF Cybersecurity Center of Excellence

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

INTERNET2

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

PITTSBURGH SUPERCOMPUTING CENTER

BERKELEY LAB

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

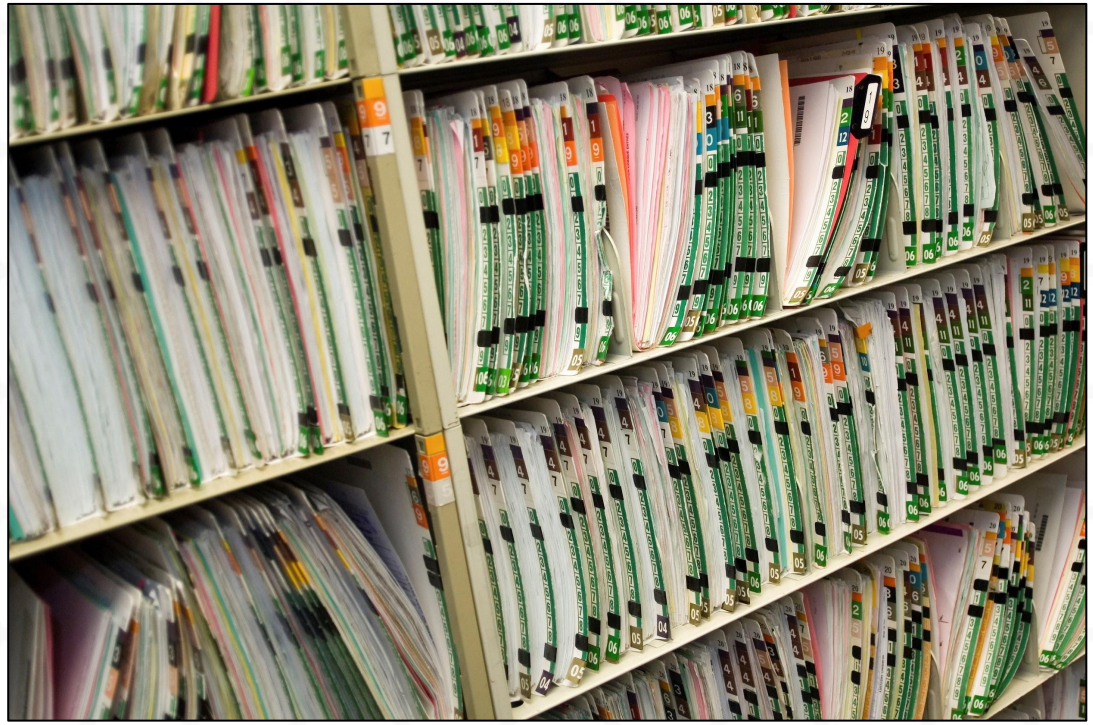
https://trustedci.org/

# My Talk

1. Why Cybersecurity for Open Science? What is unusual about cybersecurity for Open Science?
2. The NSF Cybersecurity Center of Excellence: What can it do for you?
3. Coming Attractions: ResearchSOC


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Regulated vs Open Science



Research with regulated data is guided by compliance

E.g. HIPAA, FISMA, NIST 800-171

Open science is not guided by compliance

E.g. Astronomy, climate, physics, geology

A sizeable fraction or even majority of science at a University is open

If no medical school, probably majority.

This talk focuses on open science

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Myth:
# "Open Science Does Not Need Cybersecurity"

"I don't handle confidential data, hence
I don't need cybersecurity!"


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Cybersecurity for Science Goals

Productive
Trustworthy
Reproducible

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

## Cybersecurity for Science Goals

**Productive**

Trustworthy

Reproducible

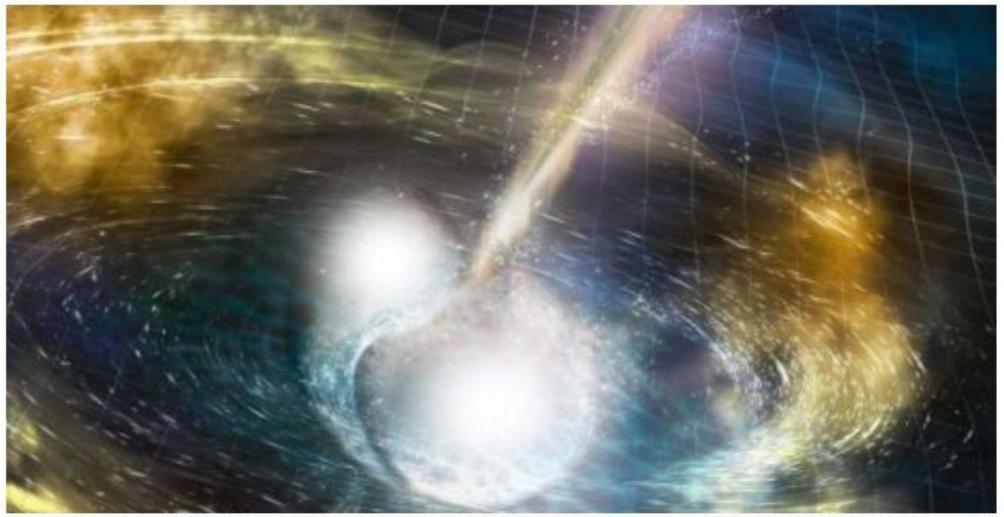
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Threat of Unavailable Instruments

## Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars

NICOLAS PERPITCH

UPDATED TUE 17 OCT 2017, 6:44 PM AEDT



0:00

VIDEO [0:30] In a galaxy 130 million lights years away two neutron stars collide

ABC NEWS

Astrophysicists at WA's Zadko telescope had just learned about the detection of a monumental deep space event involving two neutron stars colliding — which they had been hoping to find for years — when they came under sustained cyber attack.

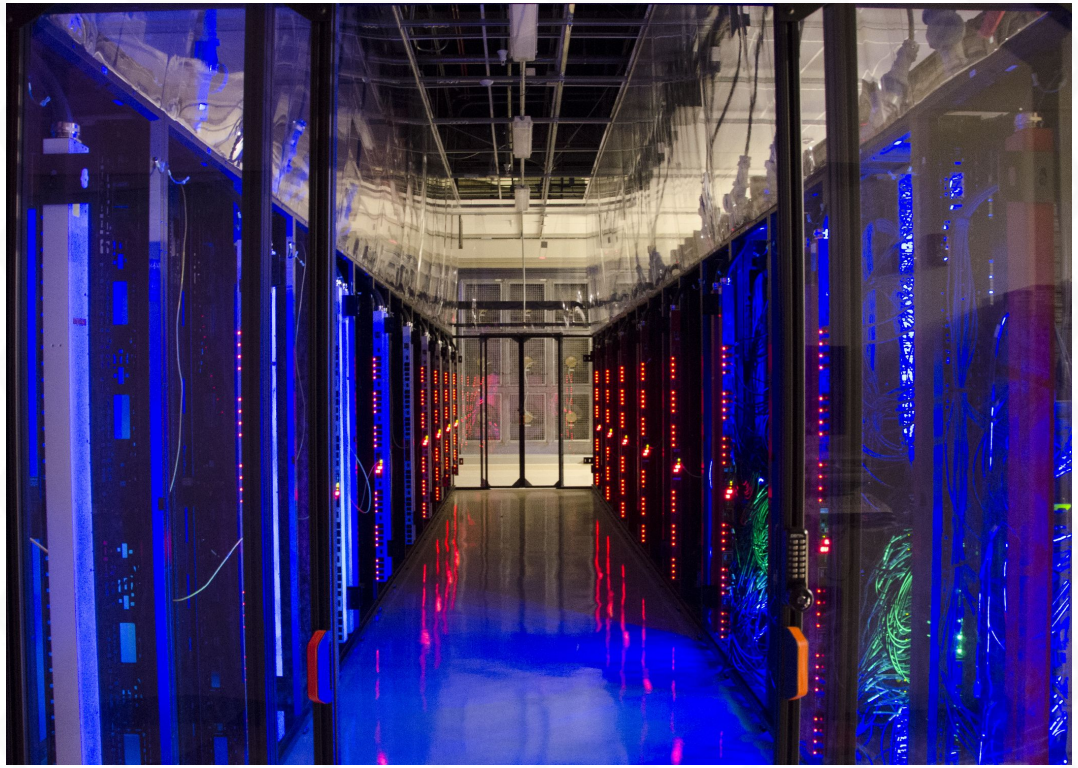
At the critical and fleeting moment, they could not move their telescope to track the gigantic explosion 130 million light years away.

http://mobile.abc.net.au/news/2017-10-17/cyber-attack-almost-costs-team-look-at-colliding-neutron-stars/9055816?pfmredir=sm

# Your Data Is Valuable to Criminals!


https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

# Cyberinfrastructure is More Diverse



!=

Credit: Chris Coleman, School of Computing, University of Utah

# Rapid, Collaborative Projects

Often short-lived (3-5 years).

Start and progress quickly.

Researcher-managed teams.

Top ten countries with most U.S. co-authors in 2015
https://www.aje.com/arc/collaboration-2015/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Cybersecurity for Science Goals

Productive

**Trustworthy**

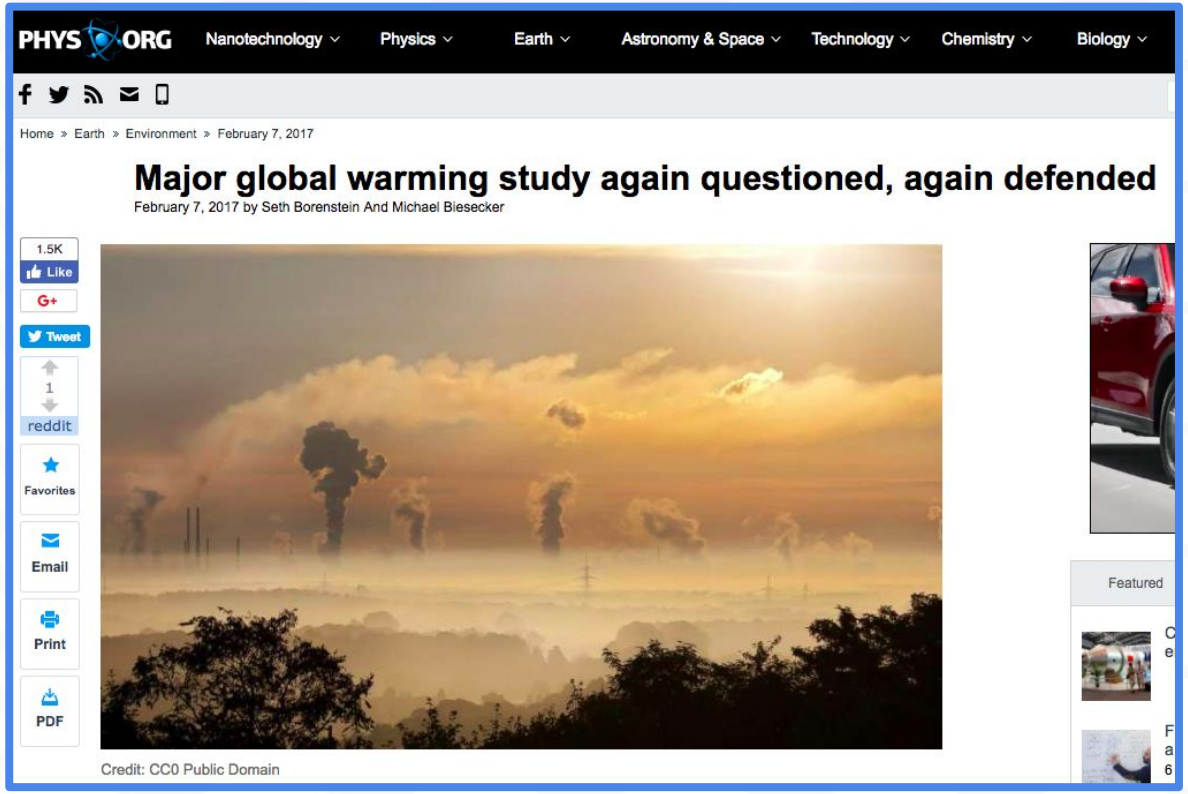
Reproducible

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Integrity First

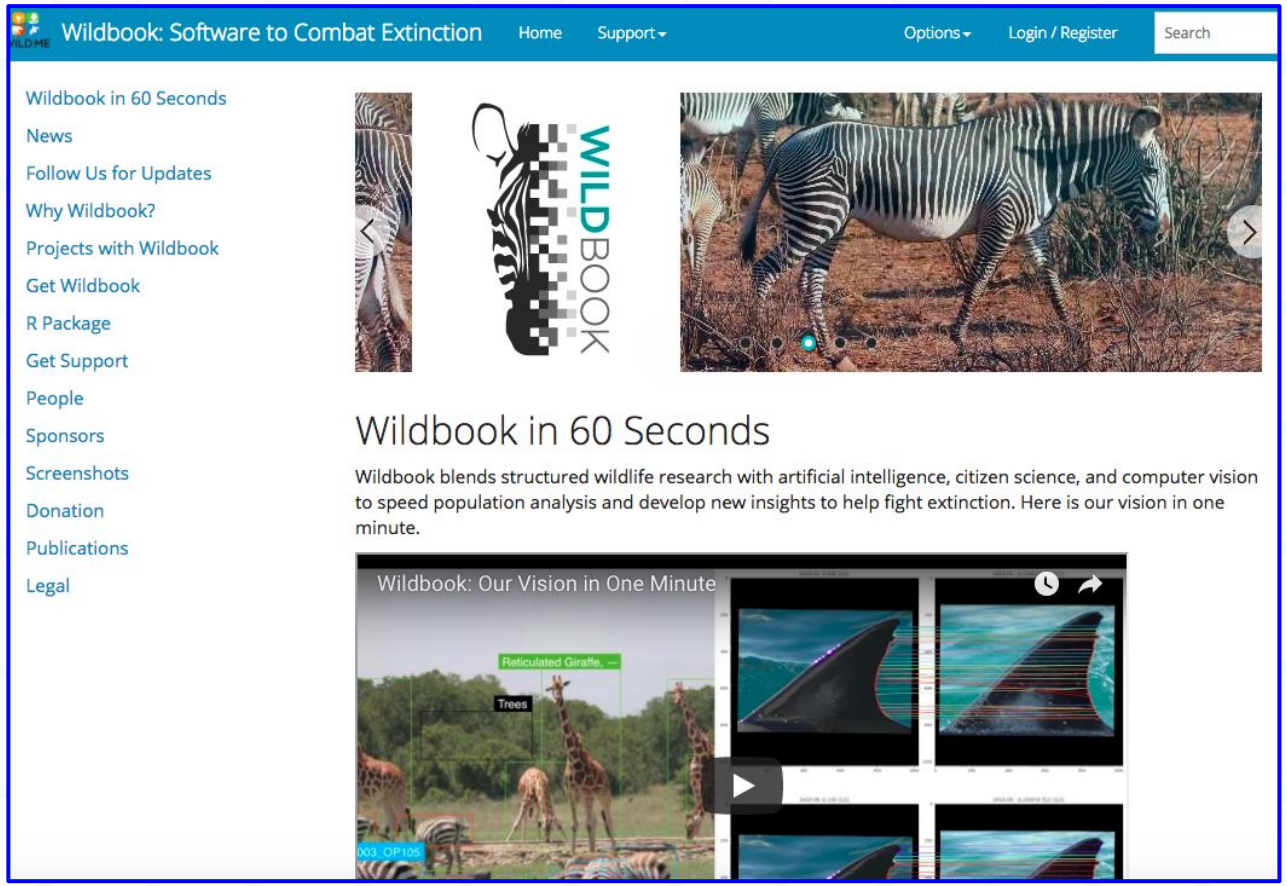
For Open Science, integrity of data is often most important aspect of cybersecurity.

Confidentiality is important for financial data, regulated data, intellectual property, etc.




https://www.cbsnews.com/news/global-warming-climate-change-study-again-questioned-again-defended/

# Ethical Concerns
# E.g. Endangered Species




http://wildbook.org/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Pre-announcement/pre-publication

## Gravitational-Wave Announcement Coming on Oct. 16: What Could It Be?

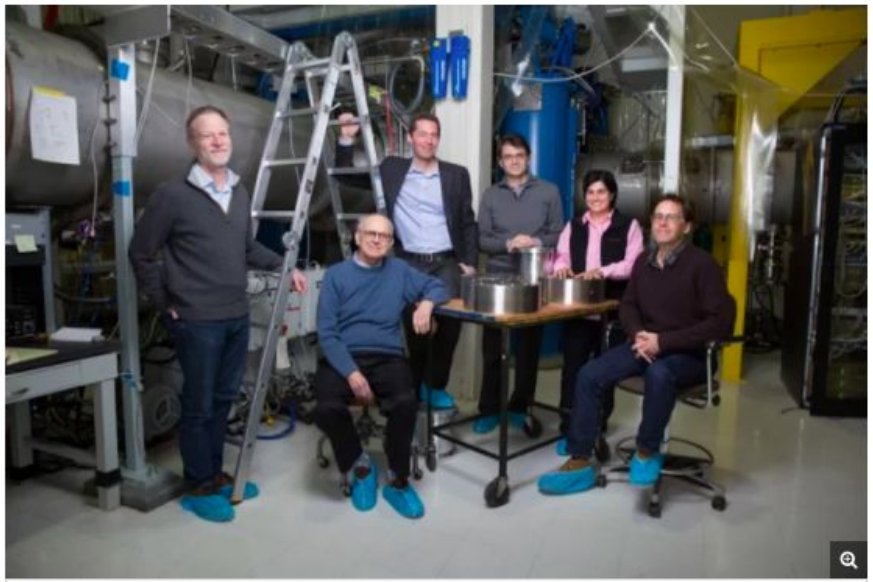
By Calla Cofield, Space.com Senior Writer | October 5, 2017 07:00am ET

138

67

MORE





Members of the MIT LIGO team (from left to right): David Shoemaker, Rainer Weiss, Matthew Evans, Erotokritos Katsavounidis, Nergis Mavalvala and Peter Fritschel. Rainer Weiss stated on Oct. 3, 2017 that the LIGO collaboration will make an exciting announcement on Oct. 16.

Credit: Bryce Vickmark/MIT

https://www.space.com/38367-gravitational-wave-announcement-coming.html

# Reputational Harm Will Erode Our Autonomy

CYBERSECURITY

## *U.S. blames 'massive' hack of research data on Iran*

Targets included nearly 8000 professors in 22 countries

*By* **Jon Cohen**

A "massive and brazen cyberassault" revealed last week by the U.S. Department of Justice (DOJ) showed that academics are easy targets for hacking. In "one of the largest state-sponsored hacking campaigns" it has ever prosecuted, DOJ alleges that nine Iranians working on behalf of the Islamic Revolutionary Guard Corps stole data from 7998 professors at 320 universities around the world over the past 5 years.

The indictment, filed by a federal grand jury in New York City and unsealed on 23 March, alleges that the hackers pilfered 31.5 terabytes of documents and data, including scientific research, journals, and dissertations. Their targets also included the United Nations, 30 U.S. companies, and five U.S. government agencies. The indictment does not name the hacked academic institutions or companies, but it notes that the victims included academic publishers, a biotechnology company, and 11 technology companies.

"This is not an isolated breach—it's hundreds if not thousands of breaches," says Anthony Ferrante, who heads cybersecurity at FTI Consulting in Washington, D.C., and formerly worked as a cyber expert for the vations behind the indictment and suggest the actual harm was modest.

According to the indictment, the attack targeted 3768 professors at 144 U.S. universities and stole data that cost the institutions about $3.4 billion to "procure and access." The accused allegedly set up an institute in Iran called Mabna that coordinated and paid for the hacks. The institute, the indictment says, aimed to "assist Iranian universities, as well as scientific and research organizations, to obtain access to non-Iranian scientific resources." The stolen data were sold through two websites, Gigapaper and Megapaper.

The indictment says the university breaches involved "spearfishing," in which the accused sent emails that tricked targets into providing their login credentials. The emails supposedly came from professors who had read articles by the targets and asked for access to more of their work, helpfully providing links. Clicking a link took the victim to a fake internet domain that resembled their own university's website and asked them to log in.

With the harvested credentials, documents and other resources were easy pickings. "College professors are like shooting fish in a barrel," says Max Kilger, a social psychologist at University of Texas in San

> ***"College professors are like shooting fish in a barrel."***
> **Max Kilger**, University of Texas



U.S. HOUSE OF REPRESENTATIVES
COMMITTEE REPOSITORY

Calendar Committees Document Search

**Hearing: Scholars or Spies: Foreign Plots Targeting America's Research and Development**

Subcommittee on Oversight (Committee on Science, Space, and Technology)

Wednesday, April 11, 2018 (10:00 AM)

**2318 RHOB**
Washington, D.C.

https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108175
http://science.sciencemag.org/content/sci/359/6383/1450.full.pdf

## Cybersecurity for Science Goals

Productive
Trustworthy
**Reproducible**

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NEWS

The National Academies of
SCIENCES · ENGINEERING · MEDICINE

May 7, 2019

# New Report Examines Reproducibility and Replicability in Science, Recommends Ways to Improve Transparency and Rigor in Research


WASHINGTON – While computational reproducibility in scientific research is generally expected when the original data and code are available, lack of ability to replicate a previous study -- or obtain consistent results looking at the same scientific question but with different data -- is more nuanced and occasionally can aid in the process of scientific discovery, says a new congressionally mandated report from the National Academies of Sciences, Engineering, and Medicine. *Reproducibility and Replicability in Science* recommends ways that researchers, academic institutions, journals, and funders should help strengthen rigor and transparency in order to improve the reproducibility and replicability of scientific research.

**Defining Reproducibility and Replicability**

The terms "reproducibility" and "replicability" are often used interchangeably, but the report uses each term to refer to a separate concept. *Reproducibility* means obtaining consistent computational results using the same input data, computational steps, methods, code, and conditions of analysis. *Replicability* means obtaining consistent results across studies aimed at answering the same scientific question, each of which has obtained its own data.

# Running Science on a Hacked Computer

https://www.pexels.com/photo/white-dices-on-checked-wood-122427/

# Cybersecurity / Reproducibility Research Agenda

Impact of unauthorized access and errors

Patching

Confidential data and software

Cost trade-off

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

E. Deelman, V. Stodden, M. Taufer, V. Welch. “Initial Thoughts on Cybersecurity and Reproducibility.” 2nd International Workshop on Practical Reproducible Evaluation of Computer Systems. June 24th, 2019. Phoenix, AZ. (to appear)

# My Talk

1. Why Cybersecurity for Open Science? What is unusual about cybersecurity for Open Science?
2. The NSF Cybersecurity Center of Excellence: What can it do for you?
3. Coming Attractions: ReseachSOC


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Trusted CI:
# The NSF Cybersecurity Center of Excellence

Our mission: to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

INTERNET2®

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

PITTSBURGH SUPERCOMPUTING CENTER

BERKELEY LAB

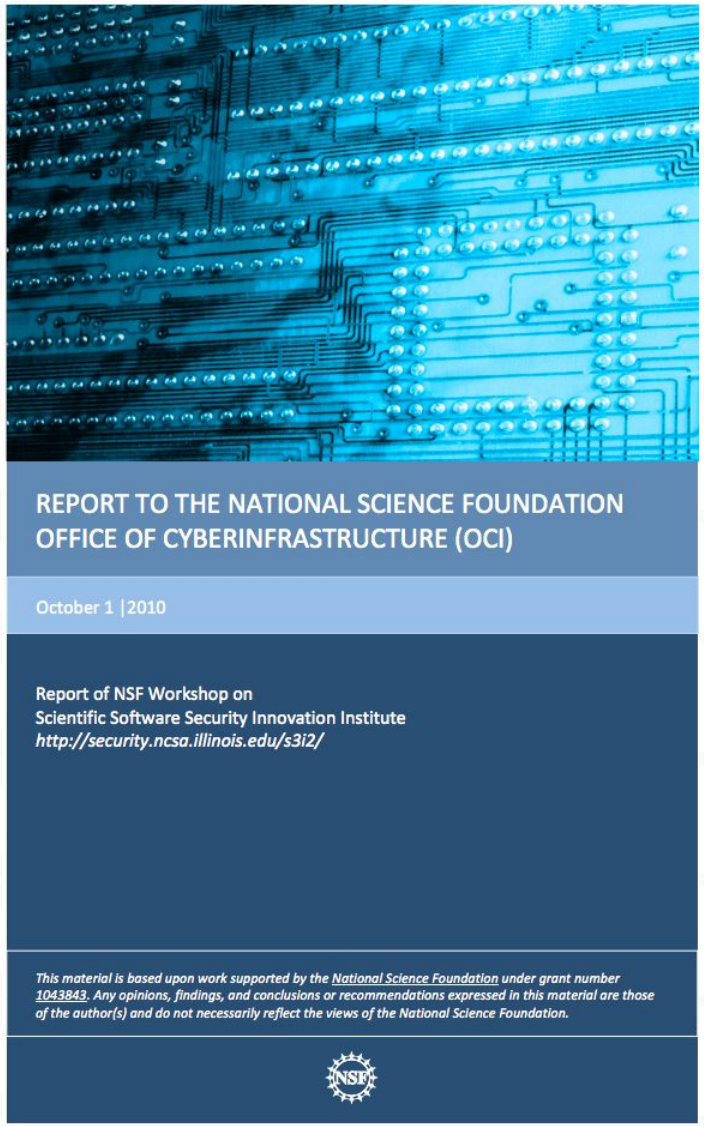
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/

# We don't make the technology. We help you make sense of it.

Formed in 2012

Based on community call for leadership and guidance rather than technology





TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

http://security.ncsa.illinois.edu/s3i2/

# Trusted CI: Impacts

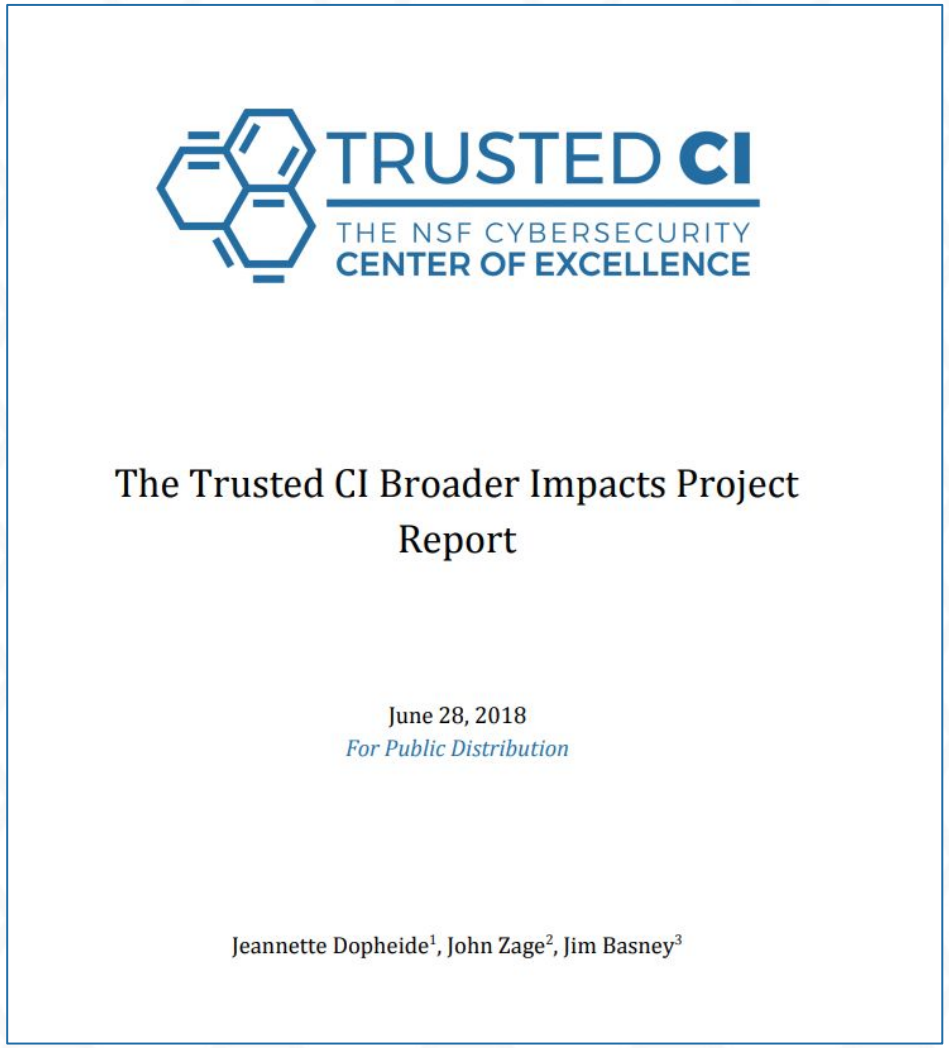
Trusted CI has impacted over 260 NSF projects since inception in 2012.

Members of more than 180 NSF projects have attended our NSF Cybersecurity Summit.

Members of more than 80 NSF projects have attended our monthly webinars.

We have provided more than 300 hours of training to the community.

We've had engagements with 41 projects, including nine NSF Large Facilities.




https://hdl.handle.net/2022/22148

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

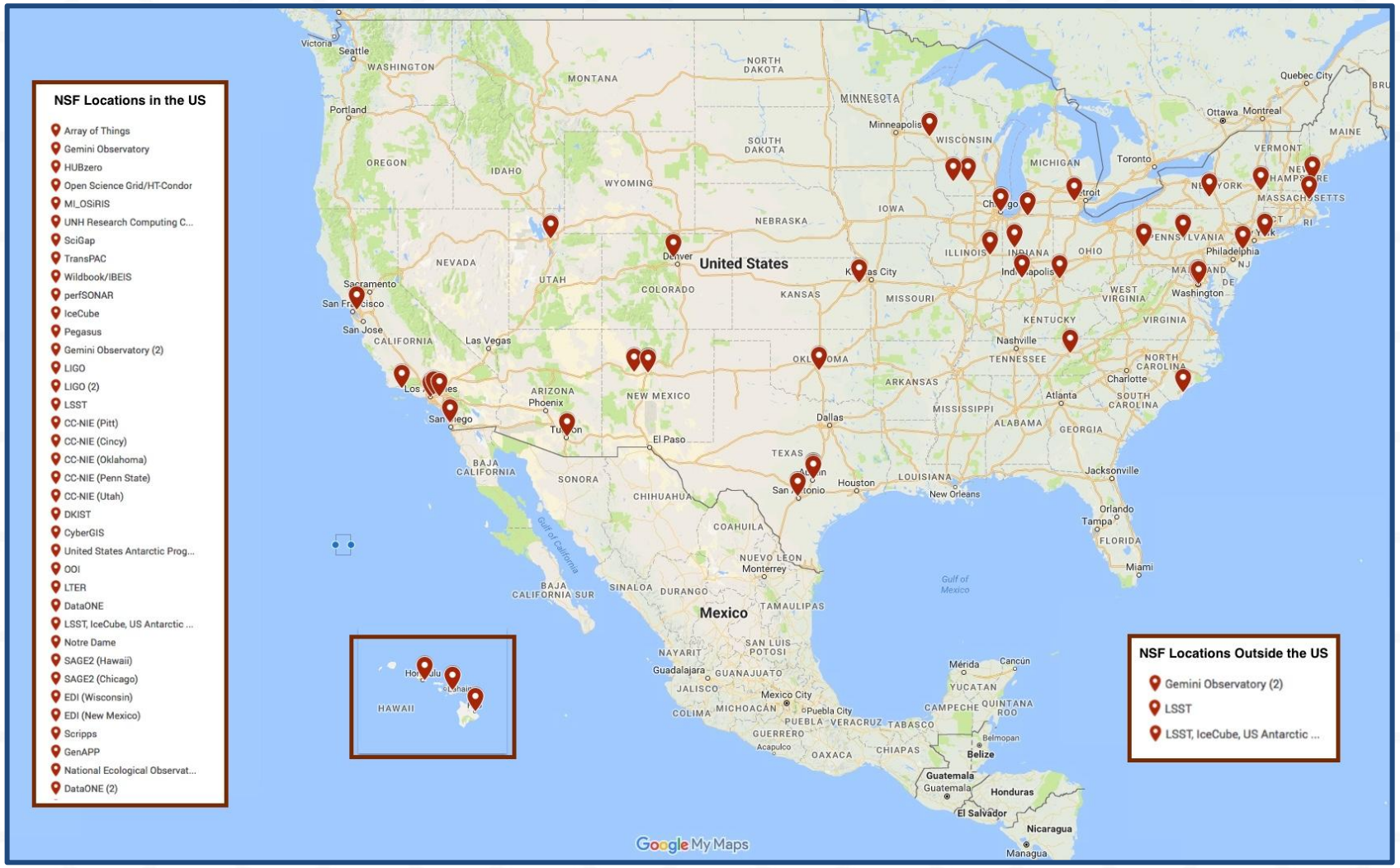
# Engagements: One-on-one Collaborations

We take applications every six months.

Accept applications every six months:

https://trustedci.org/application/

Next deadline will be Sep/Oct 2019.




TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Annual NSF Cybersecurity Summit

One day of training and workshops.

Agenda driven by call for participation.

Lessons learned and success from community.

Oct 15-17 in San Diego.

https://trustedci.org/summit/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Community-driven Guidance

Security Best Practices for Academic Cloud Service Providers

https://trustedci.org/cloud-service-provider-security-best-practices/

Operational Security

https://trustedci.org/guide

Identity Management Best Practices

https://trustedci.org/iam

Open Science Cyber Risk Profile

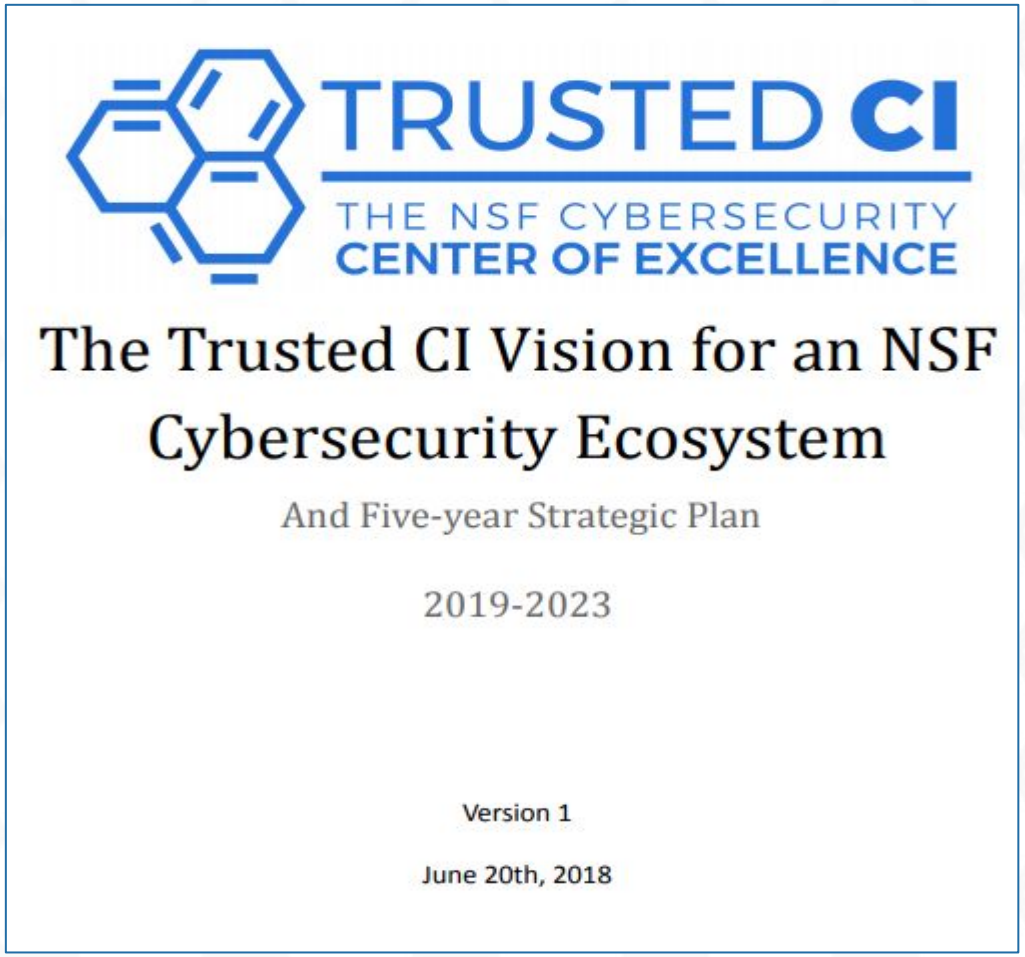
https://trustedci.org/oscrp/


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Trusted CI 5-year Vision and Strategic Plan

"A NSF cybersecurity ecosystem, formed of people, practical knowledge, processes, and cyberinfrastructure, that enables the NSF community to both manage cybersecurity risks and produce trustworthy science in support of NSF's vision of a nation that is the global leader in research and innovation."

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

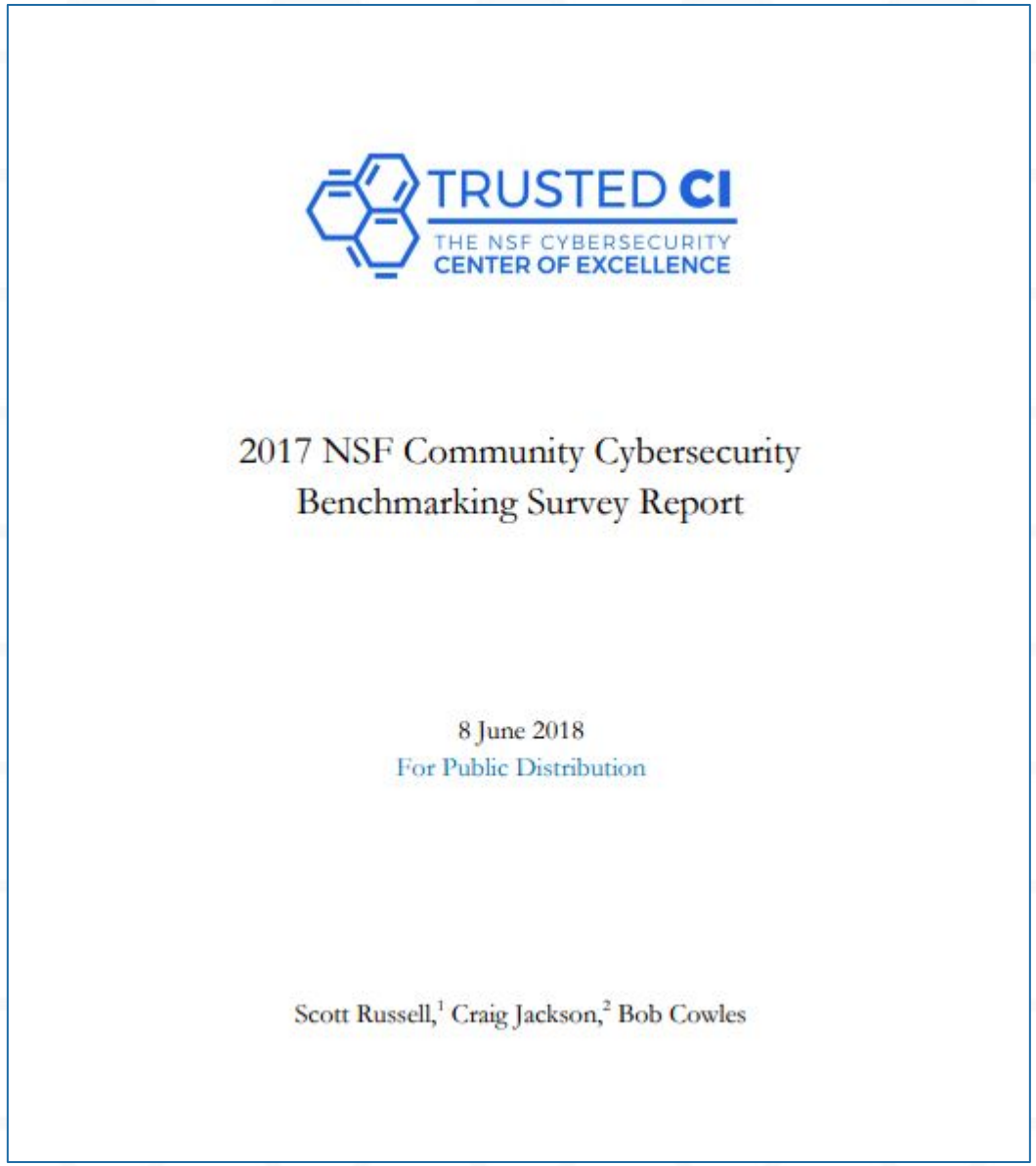



https://hdl.handle.net/2022/22178

# Community Benchmarking

Some select results:

- Respondents' cybersecurity budgets vary widely.
- Respondents inconsistently establish cybersecurity officers.
- Residual risk acceptance is inconsistently practiced.



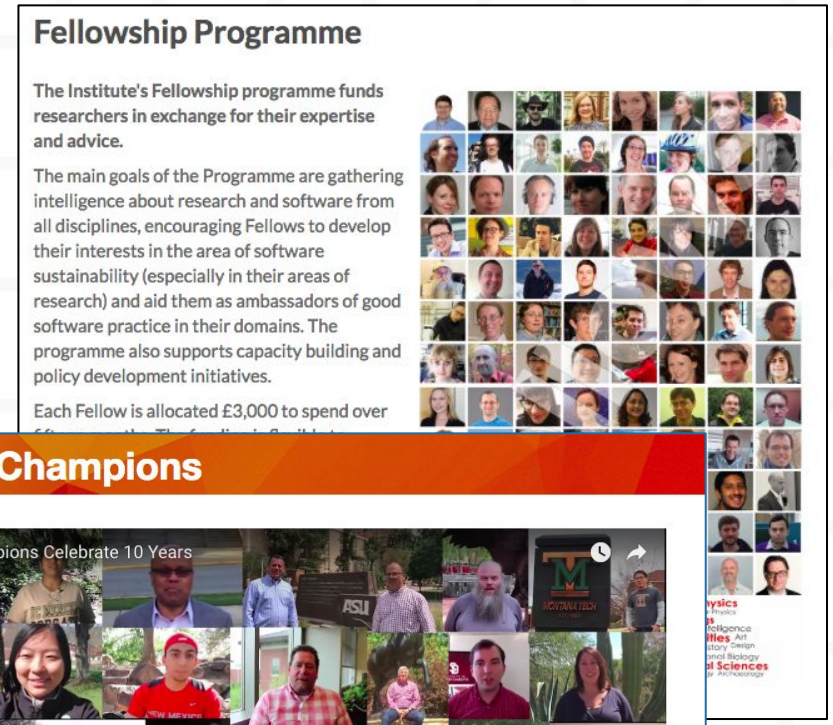

https://hdl.handle.net/2022/22171

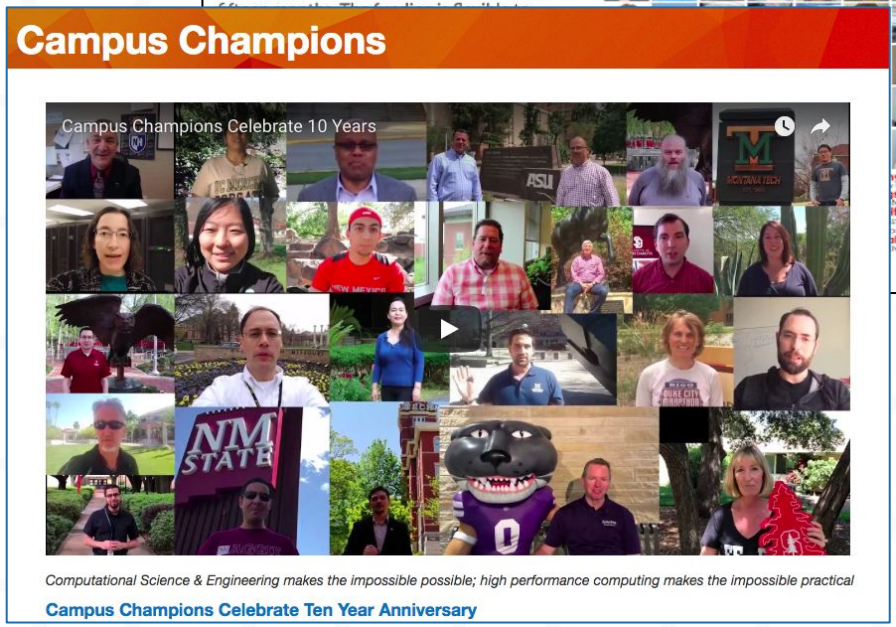
# A Network of Cybersecurity Fellows

Fellows are liaisons between Trusted CI and communities.

Fellows receive training, travel support, and prioritized support.

Building on models from UK Software Sustainability Institute, ACI-REFs, Campus Champions.




TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Cybersecurity Transition to Practice (TTP)

Enabling researcher and practitioner collaboration to accelerate cybersecurity research to practice via

- matchmaking
- business model coaching
- workshops

https://trustedci.org/ttp


2019 Cybersecurity Transition to Practice (TTP) Workshop

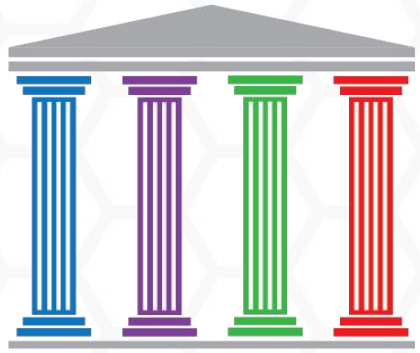
Wednesday, June 19th, 9am - 5pm. Chicago, IL

- Cybersecurity Topical Panels with Researchers and Practitioners
- Poster Session
- Thematic Co-creation breakouts for Research Transition to Practice

Request an invitation: https://trustedci.org/2019-ttp-workshop

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# The Trusted CI Framework



Framework Core:

- Concise, clear minimum requirements for cybersecurity programs organized under the 4 Pillars: Mission Alignment, Governance, Resources, and Controls
- Based in general cybersecurity best practice and evidence of what works.
- Infrequent updates.

Framework Implementation Guide:

- Guidance vetted by and tailored to the open science community.
- Curated pointers to the very best resources and tools.
- Frequent (at least yearly) updates.

Coming soon!

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Open Science Cyber Risk Profile (OSCRP)

OSCRP helps leads of science projects understand cybersecurity risks to their science and prepare for discussing those risks with their campus security office.

OSCRP was created by a team of computer security experts and scientists working together through a series of example use cases, which were then generalized to form the basis of the document.

OSCRP provides a mechanism for applying controls to mission-specific assets.

https://trustedci.org/oscrp/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Other Trusted CI Services

**Cyberinfrastructure Vulnerabilities**

Latest news on security vulnerabilities tailored for cyberinfrastructure community.

https://trustedci.org/vulnerabilities/

**Specialized Information for Identity and Access Management, Science Gateways, Software Development**

https://trustedci.org/iam/

https://trustedci.org/science-gateway-community-institute/

https://trustedci.org/software-assurance/

**Large Facilities Security Team**

Working group of security representatives from NSF Large Facilities.

https://trustedci.org/lfst/

**Ask Us Anything**

No question too big or too small.

info@trustedci.org

**Follow Us**

https://trustedci.org

https://blog.trustedci.org

@TrustedCI

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# My Talk

1. Why Cybersecurity for Open Science? What is unusual about cybersecurity for Open Science?
2. The NSF Cybersecurity Center of Excellence: What can it do for you?
3. Coming Attractions: ReseachSOC

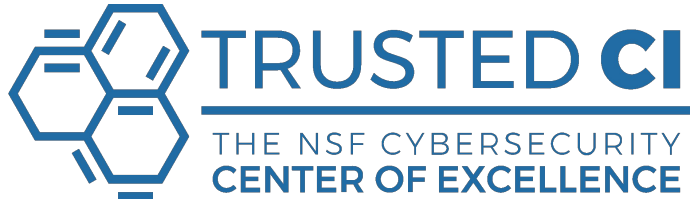

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

ResearchSOC

# Research Security Operations Center

## The second NSF-funded cybersecurity center serving the NSF science community.

# ResearchSOC complements Trusted CI


- Operational services and related training for NSF CI
- Community of Practice and Threat Intelligence Network
- Enabling Cybersecurity Research
- Outreach to Higher Ed Infosec regarding research CI

- Creating comprehensive cybersecurity programs
- Community building and leadership
- Training and best practices
- Tackling specific challenges of cybersecurity, software assurance, privacy, etc.

# ResearchSOC

PITTSBURGH SUPERCOMPUTING CENTER

UC San Diego

Operational cybersecurity services for research.

Building on existing services (OmniSOC, STINGAR) and expertise to bolster the NSF cybersecurity community's incident response capabilities.

Ramping up in 2019, initial clients in 2020, sustaining in 2021.

https://researchsoc.iu.edu/

NSF award 1840034

# Acknowledgments

Trusted CI is supported by the National Science Foundation under Grant ACI-1547272.
The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

Trusted CI activities are made possible thanks to the contributions of a multi-institutional team:

https://trustedci.org/who-we-are/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE